# Exhibit A

**CT Corporation**

**Service of Process Transmittal**
03/07/2019
CT Log Number 535055808

TO: Dawoon Kang
Coffee Meets Bagel, Inc
391 Grove St.
San Francisco, CA 94102

RE: **Process Served in Delaware**

FOR: Coffee Meets Bagel, Inc (Domestic State: DE)

**ENCLOSED ARE COPIES OF LEGAL PROCESS RECEIVED BY THE STATUTORY AGENT OF THE ABOVE COMPANY AS FOLLOWS:**

| | |
|---|---|
| **TITLE OF ACTION:** | JOHN BONELL, individually and on behalf of a class of similarly situated individuals, Pltf. vs. COFFEE MEETS BAGEL, INC., a Delaware Corporation, Dft. |
| **DOCUMENT(S) SERVED:** | Summons, Complaint |
| **COURT/AGENCY:** | COOK COUNTY - CIRCUIT COURT - CHANCERY DIVISION, IL Case # 2019CH02663 |
| **NATURE OF ACTION:** | CLASS ACTION - JURY TRIAL DEMANDED |
| **ON WHOM PROCESS WAS SERVED:** | The Corporation Trust Company, Wilmington, DE |
| **DATE AND HOUR OF SERVICE:** | By Process Server on 03/07/2019 at 12:35 |
| **JURISDICTION SERVED :** | Delaware |
| **APPEARANCE OR ANSWER DUE:** | Within 30 days after service of this Summons, not counting the day of service. |
| **ATTORNEY(S) / SENDER(S):** | Jad Sheikali MCGUIRE LAW, P.C. 55 W. Wacker Drive, 9th Fl. Chicago, IL 60601 312-893-7002 |
| **ACTION ITEMS:** | SOP Papers with Transmittal, via UPS Next Day Air , 1ZX212780111426406 |
| **SIGNED:** | The Corporation Trust Company |
| **ADDRESS:** | 1209 N Orange St Wilmington, DE 19801-1120 |
| **TELEPHONE:** | 302-658-7581 |

Page 1 of 1 / AB

Information displayed on this transmittal is for CT Corporation's record keeping purposes only and is provided to the recipient for quick reference. This information does not constitute a legal opinion as to the nature of action, the amount of damages, the answer date, or any information contained in the documents themselves. Recipient is responsible for interpreting said documents and for taking appropriate action. Signatures on certified mail receipts confirm receipt of package only, not contents.

CT

| | | |
|---|---|---|
| **2120** - Served | **2121** - Served | FILED |
| **2220** - Not Served | **2221** - Not Served | 3/1/2019 1:55 PM |
| **2320** - Served By Mail | **2321** - Served By Mail | DOROTHY BROWN |
| **2420** - Served By Publication | **2421** - Served By Publication | CIRCUIT CLERK |
| **Summons** - **Alias Summons** | **(06/28/18) CCG 0001** | COOK COUNTY, IL |
| | | 2019CH02663 |

FILED DATE: 3/1/2019 1:55 PM   2019CH02663

## IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS

JOHN BONELL, individually and for a class,

(Name all parties)      Case No. __2019-CH-02663__

v.

COFFEE MEETS BAGEL, INC., a Delaware Corp.

Coffee Meets Bagel, Inc., c/o The Corporation Trust Company Corporation Trust Center, 1209 Orange Street Wilmington, DE 19801

### ☑ SUMMONS   ☐ ALIAS SUMMONS

To each Defendant:

YOU ARE SUMMONED and required to file an answer to the complaint in this case, a copy of which is hereto attached, or otherwise file your appearance and pay the required fee **within thirty (30) days after service of this Summons**, not counting the day of service. To file your answer or appearance you need access to the internet. Please visit www.cookcountyclerkofcourt.org to initiate this process. Kiosks with internet access are available at all Clerk's Office locations. Please refer to the last page of this document for location information.

**If you fail to do so, a judgment by default may be entered against you for the relief requested in the complaint.**

To the Officer:

This Summons must be returned by the officer or other person to whom it was given for service, with endorsement of service and fees, if any, immediately after service. If service cannot be made, this Summons shall be returned so endorsed. This Summons may not be served later than thirty (30) days after its date.

**E-filing is now mandatory for documents in civil cases with limited exemptions. To e-file, you must first create an account with an e-filing service provider. Visit https://efile.illinoiscourts.gov/service-providers.htm to learn more and to select a service provider. If you need additional help or have trouble e-filing, visit http://www.illinoiscourts.gov/FAQ/gethelp.asp.**

Witness:   3/1/2019 1:55 PM DOROTHY BROWN

Atty. No.: __56618__

Atty Name: __Jad Sheikali__

Atty. for: __Plaintiff__

Address: __55 West Wacker Drive, 9th Fl.__

City: __Chicago__      State: __IL__

Zip: __60601__

Telephone: __312-893-7002__

Primary Email: __jsheikali@mcgpc.com__

Secondary Email: __dgerbie@mcgpc.com__

Tertiary Email: __emeyers@mcgpc.com__

DOROTHY BROWN, Clerk of Court

Date of Service: _____
(To be inserted by officer on copy left with Defendant or other person):

**Dorothy Brown, Clerk of the Circuit Court of Cook County, Illinois   cookcountyclerkofcourt.org**
Page 1 of 2

# CLERK OF THE CIRCUIT COURT OF COOK COUNTY OFFICE LOCATIONS

○ Richard J Daley Center
50 W Washington
Chicago, IL 60602

○ District 2 - Skokie
5600 Old Orchard Rd
Skokie, IL 60077

○ District 3 - Rolling Meadows
2121 Euclid
Rolling Meadows, IL 60008

○ District 4 - Maywood
1500 Maybrook Ave
Maywood, IL 60153

○ District 5 - Bridgeview
10220 S 76th Ave
Bridgeview, IL 60455

○ District 6 - Markham
16501 S Kedzie Pkwy
Markham, IL 60428

○ Domestic Violence Court
555 W Harrison
Chicago, IL 60607

○ Juvenile Center Building
2245 W Ogden Ave, Rm 13
Chicago, IL 60602

○ Criminal Court Building
2650 S California Ave, Rm 526
Chicago, IL 60608

## Daley Center Divisions/Departments

○ Civil Division
Richard J Daley Center
50 W Washington, Rm 601
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

◉ Chancery Division
Richard J Daley Center
50 W Washington, Rm 802
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

○ Domestic Relations Division
Richard J Daley Center
50 W Washington, Rm 802
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

○ Civil Appeals
Richard J Daley Center
50 W Washington, Rm 801
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

○ Criminal Department
Richard J Daley Center
50 W Washington, Rm 1006
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

○ County Division
Richard J Daley Center
50 W Washington, Rm 1202
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

○ Probate Division
Richard J Daley Center
50 W Washington, Rm 1202
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

○ Law Division
Richard J Daley Center
50 W Washington, Rm 801
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

○ Traffic Division
Richard J Daley Center
50 W Washington, Lower Level
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

**12-Person Jury**

FILED
2/28/2019 11:51 AM
DOROTHY BROWN
CIRCUIT CLERK
COOK COUNTY, IL
2019CH02663

*FILED DATE: 2/28/2019 11:51 AM   2019CH02663*

## CIRCUIT COURT OF COOK COUNTY, ILLINOIS
## COUNTY DEPARTMENT, CHANCERY DIVISION

| | | |
|---|---|---|
| JOHN BONELL, individually and on behalf of a class of similarly situated individuals, | ) ) ) | |
| Plaintiff, | ) ) | No. 2019CH02663 |
| v. | ) ) ) | Hon. |
| COFFEE MEETS BAGEL, INC., a Delaware corporation, | ) ) ) | |
| Defendant. | ) ) ) | JURY TRIAL DEMANDED |

### CLASS ACTION COMPLAINT & JURY DEMAND

Plaintiff John Bonell brings this Class Action Complaint and Demand for Jury Trial against

Coffee Meets Bagel, Inc., ("Defendant" or "CMB") on his own behalf, and on behalf of a class

and subclass of individuals, to seek redress for CMB's conduct leading up to, surrounding, and

following a data vulnerability and breach incident that exposed the personal information of

millions of its customers. Plaintiff alleges as follows upon personal knowledge as to himself and

his own acts and experiences, and as to all other matters, upon information and belief, including

an investigation conducted by his attorneys.

### INTRODUCTION

1.　　Coffee Meets Bagel, Inc. owns and operates a dating service via a smartphone

application called "Coffee Meets Bagel" (the "App").

2.　　CMB's App is used by millions of individuals throughout the United States. Prior

to using CMB's App, users must create a profile on the App using their full names, email addresses,

gender, registration date, and other sensitive information (collectively, "PII").

3.　　Starting in late 2017 and ending in the middle of 2018, CMB suffered a series of

data beach incidents (the "Data Vulnerability" period) concerning its App, resulting in the

1

unauthorized disclosure of the PII of over six million (6,000,000) of CMB's App customers.

4.      CMB's Data Vulnerability allowed unauthorized criminal third-parties to gain access to CMB information technology systems and extract the PII of millions of customers.

5.      Following the Data Vulnerability, the PII of millions of CMB's customers was listed for sale on the "dark web," *i.e.* the black market of the internet.

6.      Even though the Data Vulnerability was present by at least early 2017, CMB failed to reasonably detect and notify affected customers until February 2019.

7.      CMB's lax cybersecurity procedures allowed hackers to obtain access to Plaintiff's and other customers' PII. This PII should have been secured by adequate levels of protection and should not have been susceptible to unauthorized access via the Data Vulnerability.

8.      As a result of CMB's conduct in failing to reasonably prevent, detect, thwart, or mitigate the subject Data Vulnerability, Plaintiff and the other class members have suffered both pecuniary and non-pecuniary injury.

## PARTIES

9.      Defendant Coffee Meets Bagel, Inc., is a Delaware corporation that is transacting and conducting business throughout Illinois, including in Cook County. Defendant CMB intentionally targets advertisements for its products and services to residents in Illinois.

10.     At all relevant times, Plaintiff John Bonell has been a resident and citizen of the State of Illinois.

## JURISDICTION AND VENUE

11.     This Court has personal jurisdiction over Defendant pursuant to 735 ILCS 5/2-209, and in accordance with the Illinois Constitution and the Constitution of the United States, because Defendant transacts business in Illinois, including in Cook County, by soliciting and providing its

App to Illinois residents.

12.     Venue is proper in this Court because Plaintiff resides in Cook County and a substantial part of the events giving rise to the claims occurred in Cook County.

## FACTS SPECIFIC TO PLAINTIFF

13.     At all relevant times hereto, Plaintiff has been a user of the CMB App, through which he utilized CMB's online dating services.

14.     As precondition to using CMB's App, Plaintiff was required to provide his PII to CMB.

15.     On February 14, 2019, CMB sent an email to Plaintiff informing him that his PII was compromised during the Data Vulnerability. According to CMB's own email, it did not detect the Data Vulnerability until February 11, 2019, even though the Data Vulnerability existed no later than early 2017.

16.     Thus, CMB failed to detect the Data Vulnerability for no less than a year from when the Data Vulnerability first materialized.

17.     Plaintiff's PII, like that of millions of other class members, was not only compromised during the Data Vulnerability, but also listed for sale on the dark web.

18.     CMB's failure to implement reasonable cybersecurity protocols that included adequate technical, administrative, and physical controls created the subject Data Vulnerability which allowed third-party criminals to directly access Plaintiff's and other customers' PII. For example, an adequate intrusion detection and prevention system would have alerted Defendant to the presence of the of the Data Vulnerability within a reasonable time, and adequate technical measures, such as encryption, would have sufficiently de-identified the subject PII. However, CMB failed to implement such measures.

19.     Notably, Defendant not only failed to prevent the Data Vulnerability, but also failed to detect it for over a year, thereby greatly aggravated Plaintiff's and other customers' injuries and risk of identity theft.

20.     Given the current prevalence of cybersecurity awareness, especially in light of constant, high profile data breaches, CMB knew of the risks inherent in capturing, storing, and using the PII of their customers and the consequences of the exposure of such PII to unauthorized third parties.

21.     Security lapses, like the subject Data Vulnerability, harm consumers beyond increasing the likelihood of identity and financial theft—they are harmed by the fact that their personal information, such as emails, addresses, and phone numbers are connected with their names.

22.     As security experts now know, the release of data breach victims' personal information, even personal information which on its own may not constitute "traditional" PII, to the black market not only increases the likelihood of identity theft, but also makes them an easy target for spammers and phishing campaigns. Thus, Plaintiff and the Class members will be subject to imminent and ongoing, targeted, spam and phishing attacks since the third-party criminals are not only armed with certain of their PII, but also armed with the knowledge that such PII is associated with active users and valid, recently-accessed accounts.

23.     Indeed, active and valid email addresses, particularly when associated with additional user information such as first and last name, are more valuable to cyber-criminals and more easily sold to nefarious actors than "unverified" PII.

24.     Had CMB informed Plaintiff of the Data Vulnerability within a reasonable period of time following its inception, Plaintiff and the other members of the putative class would have been able to take actions to protect their PII from further misuse by identity thieves or spammers.

25.     Plaintiff believed that CMB would take reasonable measures to secure his PII. Had Plaintiff known that CMB would fail to take reasonable safeguards to protect and secure his PII, he would not have agreed to create accounts with CMB, or he would have at least acted differently upon weighing the risk in having their PII left vulnerable to attack.

26.     CMB's failure to comply with reasonable data security standards provided CMB a benefit in the form of saving on the costs of compliance, but at the expense and severe detriment of CMB's own customers, including Plaintiff, whose PII has been exposed in the Data Vulnerability, or otherwise placed at serious and ongoing risk of imminent misuse, fraudulent charges, constant spam attacks, and identity theft.

27.     Since recently becoming aware of the Data Vulnerability, Plaintiff has taken time and effort to mitigate his risk of identity theft, including changing his account passwords and monitoring his credit and other financial information to guard against fraudulent attempts to open credit cards or other financial accounts in his name.

28.     Plaintiff has also been harmed by having his PII compromised and faces the imminent and impending threat of future additional harm from the increased threat of identity theft and fraud due to his PII being sold, misappropriated, or otherwise misused by unknown parties, including ongoing spam and phishing attacks.

29.     Plaintiff has also experienced other pecuniary and non-pecuniary injury as a result of CMB's conduct leading up, surrounding, and following the breach, including mental anguish as when thinking about what would happen if his identity is stolen as a result of the Data

5

Vulnerability.

## CLASS ACTION ALLEGATIONS

30.     Plaintiff brings this action on behalf of himself and a Class and Subclass (together,

"Class" unless otherwise noted) defined as follows:

**The Class:** All individuals whose PII was in the possession of Defendant, or any of their subsidiaries and/or agents, during the Data Vulnerability.

**The Illinois Subclass:** All individuals in Illinois whose PII was in the possession of Defendant, or any of their subsidiaries and/or agents, during the Data Vulnerability.

31.     **Numerosity:** Upon information and belief there are thousands, if not more,

members of the Class. Defendant claims on its website to have made over 978,000 introductions

in 2017 in Chicago alone.[1]

32.     **Commonality and Predominance:** There are many questions of law and fact

common to the claims of Plaintiff and the other members of the putative Class, and those questions

predominate over any questions that may affect individual members of the Class. Common

questions for the Class include, but are not necessarily limited to the following:

a.      Whether CMB adequately safeguarded Plaintiff's and the Class members' PII;

b.      Whether Plaintiff and the Class members were notified of the Data Vulnerability within a reasonable period and through a reasonable method;

c.      Whether there was an unauthorized disclosure of the Class members' PII;

d.      Whether Defendant's cybersecurity prevention, detection, and notification protocols were reasonable under industry standards;

e.      Whether Defendant's PII storage and protection protocols and procedures were reasonable under industry standards;

f.      When Defendant became aware of the unauthorized access to Plaintiff's and the Class members' PII; and

---

[1] *See* Coffee Meets Bagel, *CMB Year Review: Farewell 2017, Hello 2018!*, COFFEE MEETS BAGEL BLOG, https://s3.amazonaws.com/static.cmb.com/images/Chicago_banner.jpg.

g.    Whether Defendant's conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*

33.    **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class and has retained counsel competent and experienced in complex class action. Plaintiff has no interest antagonistic to those of the other Class members, and Defendant has no defenses unique to Plaintiff.

34.    **Appropriateness**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy because joinder of all parties is impracticable. The damages suffered by the individual Class members will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual Class members to obtain effective relief from Defendant's misconduct. Even if the Class members could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action maximizes efficiencies and minimizes burdens and expenses on the parties and the judicial system.

## COUNT I
**Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act,
815 ILCS 505/1, *et seq.*
(on behalf of Plaintiff and the Illinois Subclass)**

35.    Plaintiff realleges the foregoing allegations as if fully set forth herein.

36.    Pursuant to Section 530/20 of the Illinois Consumer Fraud and Deceptive Business

Practices Act, 815 ILCS 505/1, *et seq.* ("ICFA"), Defendant was required to implement and maintain reasonable security measures to protect the Plaintiff's and the Illinois Subclass members' PII.

37.     Despite representing to Plaintiff and the Illinois Subclass members that it would not only implement commercially reasonable measures to protect their PII but also notify them if any security issues were to arise, Defendant nonetheless failed to fulfill such representations, including by failing to timely detect the Data Vulnerability.

38.     Plaintiff and the Illinois Subclass members have suffered injury in fact and actual damages, as alleged herein, as a result of Defendant's unlawful conduct and violations of the ICFA and analogous state statutes.

39.     Wherefore, Plaintiff prays for the relief set forth below.

## COUNT II
### Breach of Contract
### (on behalf of Plaintiff and the Class)

40.     Plaintiff realleges the foregoing allegations as if fully set forth herein.

41.     Plaintiff and the Class members are parties to express agreements with Defendant whereby Plaintiff and the Class members provide their PII to Defendant in exchange for the ability to create and maintain accounts with Defendant.

42.     As part of these agreements, Defendant agreed to safeguard and prevent the unauthorized disclosure of Plaintiff's and the Class members' PII.

43.     Defendant's failure to implement an adequate and reasonable data privacy and cybersecurity protocol which included adequate prevention, detection, and notification procedures constitutes a breach of contract.

44.     Defendant's failure to detect the Data Vulnerability for over a year, a gross security lapse, constitutes a separate breach of contract.

45.     Plaintiff and the Class members would not have provided and entrusted their PII to Defendant as a condition of creating their accounts with Defendant, or would have sought other alternatives with Defendant's competitors, or otherwise sought concessions, in the absence of an agreement with Defendant to reasonably safeguard their PII and to reasonably detect security issues, such as the subject Data Vulnerability.

46.     Plaintiff and the members of the Class fully performed their obligations under their contract for creating accounts with Defendant.

47.     Defendant breached the contracts it made with Plaintiff and the Class members by failing to safeguard and protect their PII and failing to reasonably and timely detect the Data Vulnerability.

48.     The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of Defendant's breaches of contract.

49.     Wherefore, Plaintiff prays for the relief set forth below.

## COUNT III
### Breach of Implied Contract
(on behalf of Plaintiff and the Class) (in the alternative to Count II)

50.     Plaintiff realleges the foregoing allegations as if fully set forth herein.

51.     Plaintiff and the Clas members were required to provide their PII to Defendant in exchange for the ability to create and maintain accounts with Defendant. To the extent that it is found that Defendant did not have an express contract with Plaintiff and the Class members, Defendant entered into implied contracts with Plaintiff and the Class members whereby, by virtue of such requirement to provide their PII, Defendant was obligated to take reasonable steps to secure

and safeguard such PII, and obligated to take reasonable steps following an unauthorized disclosure to detect the same.

52.     Defendant's failure to implement adequate and reasonable data privacy and cybersecurity protocols constitutes a breach of an implied contract between Defendant and the Class members.

53.     Plaintiff and the Class members would not have provided and entrusted their PII to Defendant in order create accounts on Defendant's website in the absence of an agreement with Defendant to reasonably safeguard their PII and to reasonably detect security issues, such as the subject Data Vulnerability.

54.     Plaintiff and the members of the Class fully performed their obligations under their implied contracts with Defendant.

55.     Defendant breached the implied contracts it made with Plaintiff and the Class members by failing to safeguard and protect their PII, and failing to reasonably and timely detect the Data Vulnerability.

56.     The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of Defendant's breaches of contract.

57.     Wherefore, Plaintiff prays for the relief set forth below

## COUNT IV
### Negligence
### (on behalf of Plaintiff and the Class)

58.     Plaintiff realleges the foregoing allegations as if fully set forth herein.

59.     As a condition of being a customer, Defendant required Plaintiff and Class members to provide their PII.

10

60.     At all relevant times, Defendant had a duty, or undertook/assumed a duty, to implement a reasonable data privacy and cybersecurity protocol, including adequate prevention, detection, and notification procedures, in order to safeguard the PII of the Plaintiff and the Class members, and to prevent the unauthorized access to and disclosures of the same.

61.     Also, upon accepting and inputting Plaintiff's and Class members' PII, Defendant undertook and owed a duty to exercise reasonable care to secure and safeguard that information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties, and to utilize commercially reasonable methods to do so. This duty included, among other things, designing, implementing, maintaining, and testing Defendant's cybersecurity systems to ensure that Plaintiff's and the Class members' PII was reasonably secured and protected.

62.     Defendant breached the aforementioned duties in, including but not limited to, one or more of the following ways:

     a.    Failing to implement reasonable data privacy and cybersecurity measures to secure its or Plaintiff's and Class members' email accounts, including failing to require adequate multifactor authentication and encryption;

     b.    Failing to implement a reasonable data privacy and cybersecurity protocol, including adequate procedures for preventing cybersecurity threats and/or detecting such threats in a timely manner;

     c.    Failing to reasonably comply with applicable state and federal law concerning its data privacy and cybersecurity protocol; and

     d.    Otherwise failing to act reasonably under the circumstances and being negligent with regards to its conduct in preventing, detecting, and disclosing the subject Data Vulnerability.

63.     Defendant knew, or should have known, that its data privacy and cybersecurity protocol failed to reasonably protect Plaintiff and the Class members' PII and failed to reasonably detect anomalies concerning the same.

64.     As a direct result of Defendant's aforesaid negligent acts and omissions, Plaintiff

and the Class members suffered injury and damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII, the loss of the benefit of their bargain in creating accounts with Defendant, and pecuniary injury in the form of expense to mitigate the disclosure and significantly increased risk of exposure of PII to nefarious third parties.

65.     Wherefore, Plaintiff prays for the relief set forth below.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class and Subclass set forth above, respectfully request the Court order relief and enter judgement against Defendant:

A.     Certifying the Class and Subclass identified above and appointing Plaintiff as Class representative and the undersigned counsel as Class counsel;

B.     Awarding Plaintiff and the Class and Subclass appropriate relief, including actual, statutory, compensatory, and/or punitive damages;

C.     Requiring Defendant to furnish identity fraud monitoring and mitigation services for a reasonable period of time;

D.     Granting injunctive relief requiring Defendant to implement commercially reasonable cybersecurity measures to properly guard against future cyberattacks and to provide prompt, reasonable notification in the event of such an attack;

E.     Requiring Defendant to pay Plaintiff's and the Class's and Subclass's reasonable attorneys' fees, expenses, and costs; and

Any such further relief as this Court deems reasonable and just.

## JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Dated: February 28, 2019

Respectfully Submitted,

JOHN BONELL, individually and on behalf of a
Class and Subclass of similarly situated individuals

By: /s/ Jad Sheikali
*One of Plaintiff's Attorneys*

Eugene Y. Turin
David L. Gerbie
Jad Sheikali
MCGUIRE LAW, P.C. (#56618)
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
eturin@mcgpc.com
dgerbie@mcgpc.com
jheikali@gmail.com

*Attorneys for Plaintiff and the Putative Class and Subclass*

13